Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016 Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

319

Vragen van de leden **Oosenbrug** en **Ypma** (beiden PvdA) aan de Staatssecretarissen van Volksgezondheid, Welzijn en Sport en van Veiligheid en Justitie over *onveilige uitwisseling van gegevens tussen gemeenten en behandelaars in de jeugd-ggz* (ingezonden 1 oktober 2015).

Antwoord van Staatssecretaris **Van Rijn** (Volksgezondheid, Welzijn en Sport) mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 19 oktober 2015).

Vraag 1
Heeft u kennisgenomen van het artikel «Gemeenten mailen onveilig over kinderen»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat behandelaars in de jeugd-ggz met een behoorlijk aantal gemeenten gegevens uitwisselen via onbeveiligde en onversleutelde kanalen? Zo ja, heeft u zicht op het aantal gemeenten dat deze informatie onbeveiligd aangeleverd wil krijgen? Zo nee, wat klopt hier niet aan?

Antwoord 2
Gemeenten en aanbieders zijn gehouden aan de wettelijke eisen die aan deze informatie-uitwisseling gesteld worden. De gemeenteraden, de Inspecties en het College bescherming persoonsgegevens (Cbp) zien hierop toe vanuit hun verschillende verantwoordelijkheden. Wij hebben geen volledig zicht op het veelzijdig berichtenverkeer tussen aanbieders en gemeenten.

Vraag 3
Heeft u kennis of ook communicatie over andere vormen van zorg, waar gemeenten verantwoordelijk voor zijn, via onbeveiligde kanalen verloopt?

[1] http://www.nrc.nl/nieuws/2015/09/23/patientinformatie-jeugdzorg-onbeveiligd-naar-gemeenten/

ah-tk-20152016-319
ISSN 0921 - 7398
’s-Gravenhage 2015

Antwoord 3
Gemeenten, politie, Veilig Thuis, de raad voor de kinderbescherming en de gecertificeerde instellingen zijn wettelijk verplicht om CORV te gebruiken voor de onderlinge uitwisseling van gegevens tussen het gemeentelijk en het justitiedomein. CORV maakt het mogelijk om tussen deze partijen op een veilige manier privacygevoelige gegevens uit te wisselen. Alle partijen maken gebruik van CORV, maar wij weten dat nog niet alle partijen dat in alle gevallen doen. Het gebruik neemt wel gestaag toe. Op dit moment vindt 65 procent van de gegevensuitwisseling plaats via CORV en er wordt hard aan gewerkt om dit percentage verder te verhogen. Wij zullen Uw Kamer in het voorjaar berichten over de voortgang.
Wij hebben geen kennis of de communicatie over andere vormen van zorg via onbeveiligde kanalen verloopt.

Vraag 4
Voldoen gemeenten door versturing via e-mail aan de wettelijk geldende eisen voor de verwerking van persoonsgegevens in de zorg? Zo nee, wordt bij dit soort situaties handhavend opgetreden, en hoeveel handhavingstrajecten lopen op dit gebied?

Antwoord 4
De wettelijke eisen zijn neergelegd in de Jeugdwet en de Wet bescherming persoonsgegevens (Wbp). Daarnaast hebben gemeenten hun eigen meer gedetailleerde norm gemaakt: de Baseline Informatiebeveiliging Gemeenten (BIG). De Informatiebeveiligingsdienst (IBD) helpt gemeenten om de BIG te implementeren. In de Buitengewone Algemene Ledenvergadering van de VNG van 29 november 2013 hebben de gemeenten de Resolutie Informatieveiligheid aangenomen. Met die resolutie hebben alle gemeenten zich verplicht om de BIG in 2017 ingevoerd te hebben.
Zie https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente en https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid.
Toezicht op de naleving van deze normen geschiedt door de gemeenteraad, het Cbp en de Inspecties. Het is aan deze partijen om te bepalen of in concrete gevallen aan de normen wordt voldaan. Wij weten dat op dit moment de Inspecties onderzoeken uitvoeren bij gemeenten en dat het Cbp de toegang onderzoekt van 41 gemeenten.

Vraag 5
Hoeveel gemeenten zijn nog niet aangesloten op het gemeentelijk gegevensknooppunt? Op welke termijn verwacht u dat alle gemeenten aangesloten zijn op het gemeentelijk gegevensknooppunt of vergelijkbare voorzieningen voor beveiligde communicatie?

Antwoord 5
Alle gemeenten zijn aangesloten op het gemeentelijk gegevensknooppunt. Aanbieders moeten daarnaast zijn aangesloten op het gegevensknooppunt van VECOZO, dat kan communiceren met het gegevensknooppunt van gemeenten. Nog niet alle aanbieders, vooral de kleinere in bijvoorbeeld de jeugd-GGZ, zijn hierop aangesloten. Via de gegevensknooppunten kunnen alleen standaardberichten worden verstuurd.
Veel gemeenten en aanbieders hebben uiteenlopende inkoopcontracten afgesloten, die aanleiding geven tot een daarop aansluitend berichtenverkeer, dat vaak wordt ondersteund door regionale ict voorzieningen. Het uitwisselen van berichten met persoonsgegevens komt met name voor bij «prijs per product» afspraken, zoals beoogd in de overgangsperiode van de jeugd GGZ naar de brede jeugdhulp 2015–2017. Echter, ook voor jeugd GGZ zijn er gemeenten die in 2015 andere inkoopmodellen hebben gehanteerd dan de «prijs per product» benadering, d.w.z. de DBC bekostiging. Positief is dat gemeenten werk maken van lokaal maatwerk en dat bij het toepassen van andere dan «prijs per product» afspraken minder persoonsgegevens behoeven te worden uitgewisseld. Dit leidt er wel toe dat toezicht op veilig berichtenverkeer ook maatwerk zal zijn.

Vraag 6
Deelt u de zorg van de behandelaars dat gemeenten hen geen garanties of informatie kunnen geven voor een zorgvuldige omgang met gevoelige gegevens die zij moeten verstrekken? Op welke informatie over de verwerking hebben behandelaars en cliënten recht?

Antwoord 6
Nee, deze zorg delen wij niet. De wettelijke kaders zijn duidelijk. Ook is duidelijk welke gemeentelijke normen, BIG, er gelden. Gemeenten dienen zich aan die regels te houden; de gemeenteraad, het Cbp en de Inspecties zien hierop toe.
In de tijdelijke regeling over de bij de declaratie te verstrekken persoonsgegevens is limitatief opgesomd waar de gemeenten de ontvangen gegevens voor mogen gebruiken, te weten voor de formele controle, voor het opvragen van nadere informatie bij de declarant indien de ingediende rekening te weinig informatie bevat om hem te kunnen betalen, voor het betalen van de rekening, voor fraudeonderzoek en voor de vaststelling van ouderbijdragen. De informatie mag dus bijvoorbeeld niet worden gebruikt om te bepalen of aansluitend andere jeugdhulp nodig zou kunnen zijn. Uiteraard kunnen de gemeenten de aanbieders hiervan op de hoogte stellen. Evenzo kan een gemeente dit desgevraagd meedelen aan een jeugdige of zijn ouders.
Voorts heeft de gemeente op grond van artikel 33 en 34 Wbp een informatieplicht. Zij moet op eigen initiatief de betrokkenen in ieder geval op de hoogte stellen van het bestaan en het doel van de gegevensverwerking door middel van brochures en folders.

Vraag 7
Op welke manier wordt de stand van zaken van de veiligheid en kwaliteit van de informatiesystemen van gemeenten op het gebied van het sociale domein gemonitord? Hoe wordt vervolgens gewerkt aan verbetering?

Antwoord 4
De veiligheid en kwaliteit van de informatiesystemen van gemeenten wordt gemonitord per gemeente via waarstaatjegemeente.nl (http://www.waarstaatjegemeente.nl/dashboard/Rapporten--c53/).
De gemeenten werken aan verbetering door de hiervoor genoemde verplichte implementatie van de Baseline Informatieveiligheid Gemeenten per 2017.
Daarnaast verzorgen Rijk en VNG gezamenlijk thans een serie masterclasses Privacy sociaal domein en Jeugd, om gemeenten te equiperen om de zorgvuldige omgang met gevoelige gegevens te borgen.
Voorts worden gemeenten ondersteund vanuit Programma Informatievoorziening Sociaal Domein (ISD) (https://www.visd.nl/visd/gegevensuitwisseling-en-privacy) en de IBD (https://www.ibdgemeenten.nl/ of https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid).